

## **AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

- 1      1. (Currently amended) A computer controlled method to construct a secure credential infrastructure comprising steps of:
  - 3                exchanging key commitment information over a preferred channel between a credential issuing device and a prospective member device to pre-authenticate said prospective member device, wherein said preferred channel has both a demonstrative identification property and an authenticity property;
  - 7                receiving a public key from said prospective member device;
  - 8                verifying said public key with said key commitment information; and
  - 9                automatically provisioning said prospective member device with a credential authorized by a credential issuing authority.
- 1      2. (Original) The computer controlled method of claim 1, further comprising establishing proof that said prospective member device is in possession of a private key corresponding to said public key.
- 1      3. (Original) The computer controlled method of claim 2, further comprising establishing a communication channel between said prospective member device and said credential issuing authority responsive to the step of establishing proof.
- 1      4. (Original) The computer controlled method of claim 3, wherein said credential is secret and said communication channel is a secure communication channel.

- 1       5. (Original) The computer controlled method of claim 1, further comprising configuring  
2                    said credential issuing authority.
- 1       6. (Original) The computer controlled method of claim 1, wherein said credential issuing  
2                    device includes said credential issuing authority.
- 1       7. (Original) The computer controlled method of claim 1, wherein the step of exchanging  
2                    further comprises sending network configuration information to said prospective  
3                    member device.
- 1       8. (Original) The computer controlled method of claim 1, wherein the step of  
2                    automatically provisioning further comprises steps of:  
3                          determining provisioning information for said prospective member device; and  
4                          sending said provisioning information to said prospective member device.
- 1       9. (Original) The computer controlled method of claim 8, wherein said provisioning  
2                    information further comprises application-specific configuration information.
- 1       10. (Original) The computer controlled method of claim 1, wherein said preferred channel  
2                    is a location-limited channel.
- 1       11. (Original) The computer controlled method of claim 1, wherein said preferred channel  
2                    uses a telephone switching system.
- 1       12. (Canceled).
- 1       13. (Original) The computer controlled method of claim 1, wherein said key commitment  
2                    information is selected from one or more of the group consisting of a portion of said  
3                    public key, said public key, an encoding of said public key, and a mathematical  
4                    function of said public key.

- 1       14. (Original) The computer controlled method of claim 1, wherein the step of  
2                  automatically provisioning is performed by said credential issuing device.
- 1       15. (Original) The computer controlled method of claim 1, wherein the step of  
2                  automatically provisioning is performed by an enrollment station in communication  
3                  with said credential issuing device.
- 1       16. (Original) The computer controlled method of claim 15, wherein the method further  
2                  comprises establishing secure communication between said enrollment station and  
3                  said credential issuing device.
- 1       17. (Original) The computer controlled method of claim 1, wherein said prospective  
2                  member device is selected from one or more of the group consisting of a computer,  
3                  a personal data assistant, a smart card, a cryptographic token, a medical device, a  
4                  device containing personal information, a secure telephone, a cell telephone, a  
5                  vehicle, a container, an access card, a biometric sensor, a wireless network device, a  
6                  proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device  
7                  capable of receiving a credential, a device capable of issuing a credential.
- 1       18. (Original) The computer controlled method of claim 1, wherein said secure credential  
2                  infrastructure is a public key infrastructure, said credential issuing authority is a  
3                  certification authority and said credential is a public key certificate.
- 1       19. (Original) The computer controlled method of claim 18, wherein the step of  
2                  automatically provisioning further comprises steps of:  
3                          determining provisioning information for said prospective member device;  
4                          creating a public key certificate as said credential responsive to said  
5                  provisioning information; and  
6                          sending said public key certificate to said prospective member device.

1       20. (Original) The computer controlled method of claim 18, wherein the step of  
2            exchanging further comprises steps of:  
3              creating a public key pair for said prospective member device; and  
4              sending said public key pair to said prospective member device over said preferred  
5              channel.

1       21. (Original) The computer controlled method of claim 18, further comprises steps of:  
2              creating a trusted key pair;  
3              storing said trusted key pair;  
4              establishing a certification authority public key certificate; and  
5              storing said certification authority public key certificate.

1       22. (Original) The computer controlled method of claim 21, wherein the step of  
2            automatically provisioning is responsive to authorization from a registration agent.

1       23. (Currently amended) A computer-readable storage medium storing instructions that  
2            when executed by a computer cause the computer to perform a method to construct  
3            a secure credential infrastructure, the method comprising steps of:  
4              exchanging key commitment information over a preferred channel between a  
5              credential issuing device and a prospective member device to pre-authenticate said  
6              prospective member device, wherein said preferred channel has both a  
7              demonstrative identification property and an authenticity property;  
8              receiving a public key from said prospective member device;  
9              verifying said public key with said key commitment information; and

10                   automatically provisioning said prospective member device with a credential  
11                   authorized by a credential issuing authority.

1       24. (Original) The computer-readable storage medium of claim 23, wherein said public  
2                   key is received over said preferred channel.

1       25. (Original) The computer-readable storage medium of claim 23, wherein the step of  
2                   automatically provisioning further comprises steps of:

3                   determining provisioning information for said prospective member device; and  
4                   sending said provisioning information to said prospective member device.

1       26. (Original) The computer-readable storage medium of claim 23, wherein the step of  
2                   exchanging is initiated by said prospective member device.

1       27. (Original) The computer-readable storage medium of claim 23, wherein the step of  
2                   exchanging is initiated by said credential issuing device.

1       28. (Original) The computer-readable storage medium of claim 23, wherein the step of  
2                   automatically provisioning is performed by said credential issuing device.

1       29. (Original) The computer-readable storage medium of claim 23, wherein said  
2                   prospective member device is selected from one or more of the group consisting of  
3                   a computer, a personal data assistant, a smart card, a cryptographic token, a  
4                   medical device, a device containing personal information, a secure telephone, a cell  
5                   telephone, a vehicle, a container, an access card, a biometric sensor, a wireless  
6                   network device, a proximity sensor, a sensor device, traffic sensor, an alarm device,  
7                   a robot, a device capable of receiving a credential, a device capable of issuing a  
8                   credential.

- 1       30. (Original) The computer-readable storage medium of claim 23, wherein said secure  
2            credential infrastructure is a public key infrastructure, said credential issuing  
3            authority is a certification authority and said credential is a public key certificate.
- 1       31. (Currently amended) A credential issuing apparatus configured to construct a secure  
2            credential infrastructure comprising:  
3                  at least one port configured to establish a preferred channel, wherein said  
4                  preferred channel has both a demonstrative identification property and an  
5                  authenticity property;  
6                  a key commitment receiver mechanism configured to receive key commitment  
7                  information ~~through said at least one port over said preferred channel~~;  
8                  a key receiver mechanism configured to receive a public key;  
9                  a pre-authentication mechanism configured to verify said public key with said  
10                 key commitment information; and  
11                  a credential provisioning mechanism configured to be able to automatically  
12                 provide a credential authorized by a credential issuing authority responsive to the  
13                 pre-authentication mechanism.
- 1       32. (Original) The apparatus of claim 31, wherein said public key is received over said  
2            preferred channel.
- 1       33. (Original) The apparatus of claim 31, further comprising a key-pair validation  
2            mechanism configured to establish proof that a prospective member device is in  
3            possession of a private key corresponding to said public key.
- 1       34. (Original) The apparatus of claim 31, further comprising an initialization mechanism  
2            configured to configure said credential issuing authority.

1       35. (Original) The apparatus of claim 31, wherein said credential issuing device further  
2                   comprises said credential issuing authority.

1       36. (Original) The apparatus of claim 31, further comprises a network device  
2                   configuration mechanism configured to send network configuration information  
3                   over said preferred channel.

1       37. (Original) The apparatus of claim 31, wherein the credential provisioning mechanism  
2                   further comprises:

3                   a determination mechanism configured to determine provisioning information  
4                   for said prospective member device; and

5                   a transmission mechanism configure to send said provisioning information to  
6                   said prospective member device.

1       38. (Original) The apparatus of claim 31, wherein said key commitment information is  
2                   selected from the group consisting of a portion of said public key, said public key,  
3                   an encoding of said public key, and a mathematical function of said public key.

1       39. (Original) The apparatus of claim 31, wherein the credential issuing device is an  
2                   enrollment station capable of being in communication with said credential issuing  
3                   authority.

1       40. (Original) The apparatus of claim 33, wherein said prospective member device is  
2                   selected from one or more of the group consisting of a computer, a personal data  
3                   assistant, a smart card, a cryptographic token, a medical device, a device  
4                   containing personal information, a secure telephone, a cell telephone, a vehicle, a  
5                   container, an access card, a biometric sensor, a wireless network device, a  
6                   proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device  
7                   capable of receiving a credential, a device capable of issuing a credential.

1       41. (Original) The apparatus of claim 31, wherein said secure credential infrastructure is a  
2                   public key infrastructure, said credential issuing authority is a certification authority  
3                   and said credential is a public key certificate.

1       42. (Original) The apparatus of claim 41, wherein the credential provisioning mechanism  
2                   further comprises:

3                        a services determination mechanism capable of determining provisioning  
4                        information for a prospective member device;

5                        a certificate creation mechanism configured to create a public key certificate as  
6                        said credential responsive to said provisioning information; and

7                        a sending mechanism capable of sending said public key certificate to said  
8                        prospective member device.

1       43. (Original) The apparatus of claim 41, wherein the key commitment receiver  
2                   mechanism further comprises:

3                        a key creation mechanism capable of creating a public key pair for a  
4                        prospective member device; and

5                        a sending mechanism capable of sending said public key pair to said  
6                        prospective member device over said preferred channel.

1       44. (Original) The apparatus of claim 41, further comprising an automatic configuration  
2                   mechanism comprising:

3                        a key pair creation mechanism configured to create a trusted key pair;

4                        a key pair storage mechanism configured to store said trusted key pair;

5                        a public key certificate generation mechanism configured to establish a  
6                        certification authority public key certificate responsive to said trusted key pair; and

7                   a certificate storage mechanism configured to store said certification authority  
8                   public key certificate.

1       45. (Original) The apparatus of claim 44, wherein the public key certificate generation  
2                   mechanism further comprises a parent CA receiver mechanism configured to  
3                   receive said certification authority public key certificate from a parent certification  
4                   authority.

1       46. (Original) A credential issuing apparatus configured to construct a secure credential  
2                   infrastructure comprising:

3                   at least one port configured to establish a preferred channel;

4                   a key commitment receiver mechanism configured to receive commitment  
5                   information for a secret through said at least one port;

6                   a key receiver mechanism configured to receive said secret;

7                   a pre-authentication mechanism configured to verify said secret with said  
8                   commitment information; and

9                   a credential provisioning mechanism configured to be able to automatically  
10                  provide a credential authorized by a credential issuing authority responsive to the  
11                  pre-authentication mechanism.

12

1       47. (Currently amended) A computer controlled method to join a prospective member  
2                   device with a secure credential infrastructure comprising steps of:

3                   exchanging key commitment information over a preferred channel between a  
4                   credential issuing device and said prospective member device, wherein said  
5                   preferred channel has both a demonstrative identification property and an  
6                   authenticity property;

7 receiving a public key by said prospective member device;  
8 verifying said public key with said key commitment information; and  
9 receiving a credential authorized by a credential issuing authority.

1 48. (Original) The computer controlled method of claim 47, further comprising  
2 establishing proof that said credential issuing device is in possession of a private  
3 key corresponding to said public key.

1 49. (Original) The computer-controlled method of claim 48, further comprising  
2 establishing a communication channel between said prospective member device and  
3 said credential issuing authority responsive to the step of establishing proof.

1 50. (Original) The computer controlled method of claim 47, wherein said secure credential  
2 infrastructure is a public key infrastructure, said credential issuing authority is a  
3 certification authority and said credential is a public key certificate.

1 51. (Original) The computer controlled method of claim 47, wherein said preferred  
2 channel is a location-limited channel.

1 52. (Original) The computer controlled method of claim 47, wherein said preferred  
2 channel uses a telephone switching system.

1 53. (Canceled).

1 54. (Original) The computer controlled method of claim 47, wherein the step of  
2 exchanging is initiated by said prospective member device.

1 55. (Original) The computer controlled method of claim 47, wherein the step of  
2 exchanging is initiated by said credential issuing device.

1       56. (Original) The computer controlled method of claim 47, wherein said key commitment  
2                   information comprises a portion of said public key.

1       57. (Original) The computer controlled method of claim 47, wherein said key commitment  
2                   information comprises a function of said public key.

1       58. (Original) The computer controlled method of claim 50, further comprising receiving a  
2                   public key pair by said prospective member device.

1       59. (Original) The computer controlled method of claim 47, further comprising receiving  
2                   provisioning information by said prospective member device.

1       60. (Original) The computer controlled method of claim 47, wherein said prospective  
2                   member device is selected from one or more of the group consisting of a computer,  
3                   a personal data assistant, a smart card, a cryptographic token, a medical device, a  
4                   device containing personal information, a secure telephone, a cell telephone, a  
5                   vehicle, a container, an access card, a biometric sensor, a wireless network device, a  
6                   proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device  
7                   capable of receiving a credential, a device capable of issuing a credential.

1       61. (Currently amended) A computer-readable storage medium storing instructions that  
2                   when executed by a computer cause the computer to join a prospective member  
3                   device with a secure credential infrastructure, the method comprising steps of:

4                   exchanging key commitment information over a preferred channel between a  
5                   credential issuing device and said prospective member device, wherein said  
6                   preferred channel has both a demonstrative identification property and an  
7                   authenticity property;

8                   receiving a public key by said prospective member device;

9 verifying said public key with said key commitment information; and

10 receiving a credential authorized by a credential issuing authority.

1 62. (Original) The computer-readable storage medium of claim 61, wherein said preferred  
2 channel uses a telephone switching system.

1 63. (Original) The computer-readable storage medium of claim 61, wherein the step of  
2 exchanging is initiated by said prospective member device.

1 64. (Original) The computer-readable storage medium of claim 61, wherein the step of  
2 exchanging is initiated by said credential issuing device.

1 65. (Original) The computer-readable storage medium of claim 61, wherein said key  
2 commitment information comprises a function of said public key.

1 66. (Original) The computer-readable storage medium of claim 61, wherein said  
2 prospective member device is selected from one or more of the group consisting of  
3 a computer, a personal data assistant, a smart card, a cryptographic token, a  
4 medical device, a device containing personal information, a secure telephone, a cell  
5 telephone, a vehicle, a container, an access card, a biometric sensor, a wireless  
6 network device, a proximity sensor, a sensor device, traffic sensor, an alarm device,  
7 a robot, a device capable of receiving a credential, a device capable of issuing a  
8 credential.

9

1 67. (Currently amended) An apparatus capable of joining a secure credential infrastructure  
2 comprising:

3               at least one port configured to establish a preferred channel, wherein said  
4               preferred channel has both a demonstrative identification property and an  
5               authenticity property;

6               a key commitment receiver mechanism configured to receive key commitment  
7               information ~~through~~over said preferred channel~~at least one port~~;

8               a key receiver mechanism configured to receive a public key;

9               a pre-authentication mechanism configured to verify said public key with said  
10              key commitment information; and

11              a credential receiving mechanism configured to receive a credential responsive  
12              to the pre-authentication mechanism.

1       68. (Original) The apparatus of claim 67, further comprising a key-pair validation  
2              mechanism configured to establish proof that a credential issuing device is in  
3              possession of a private key corresponding to said public key.

1       69. (Original) The apparatus of claim 68, further comprising a network interface  
2              configured to establish a communication channel with a credential issuing authority  
3              responsive to the key-pair validation mechanism.

1       70. (Original) The apparatus of claim 67, wherein said secure credential infrastructure is a  
2              public key infrastructure, said credential issuing authority is a certification authority  
3              and said credential is a public key certificate.

1       71. (Original) The apparatus of claim 67, wherein said preferred channel is a location-  
2              limited channel.

1       72. (Canceled).

- 1       73. (Original) The apparatus of claim 67, wherein said key commitment information  
2                   comprises a portion of said public key.
- 1       74. (Original) The apparatus of claim 67, wherein said key commitment information  
2                   comprises a function of said public key.
- 1       75. (Original) The apparatus of claim 70, further comprising a receiving mechanism  
2                   capable of receiving a public key pair.
- 1       76. (Original) The apparatus of claim 67, further comprising a receiving mechanism  
2                   capable of receiving provisioning information.
- 1       77. (Original) The apparatus of claim 67, further including one or more components  
2                   selected from the group consisting of a computer, a personal data assistant, a smart  
3                   card, a cryptographic token, a medical device, a device containing personal  
4                   information, a secure telephone, a cell telephone, a vehicle, a container, an access  
5                   card, a biometric sensor, a wireless network device, a proximity sensor, a sensor  
6                   device, traffic sensor, an alarm device, a robot, a device capable of receiving a  
7                   credential, a device capable of issuing a credential.
- 1       78. (New) A computer controlled method to construct a secure credential infrastructure  
2                   comprising steps of:  
3                         exchanging key commitment information over a preferred channel between a  
4                         credential issuing device and a prospective member device to pre-authenticate said  
5                         prospective member device;  
6                         sending network configuration information over said preferred channel to said  
7                         prospective member device;  
8                         receiving a public key from said prospective member device;  
9                         verifying said public key with said key commitment information; and

10                   automatically provisioning said prospective member device with a credential  
11                   authorized by a credential issuing authority.

1       79. (New) A computer-readable storage medium storing instructions that when executed  
2                   by a computer cause the computer to perform a method to construct a secure  
3                   credential infrastructure, the method comprising steps of:

4                   exchanging key commitment information over a preferred channel between a  
5                   credential issuing device and a prospective member device to pre-authenticate said  
6                   prospective member device;

7                   sending network configuration information over said preferred channel to said  
8                   prospective member device;

9                   receiving a public key from said prospective member device;

10                  verifying said public key with said key commitment information; and

11                  automatically provisioning said prospective member device with a credential  
12                  authorized by a credential issuing authority.